Autori e vittime nella criminalità informatica

Antonio Apruzzese•

Riassunto
Il crimine informatico è oggi sempre più decisamente appannaggio di nuove imprese criminali transnazionali caratterizzate da nuovi modelli di costituzione, di arruolamento di adepti e di riciclaggio. Le nuove fenomenologie criminali che attingono alle sempre più sofisticate tecnologie dell'informatica rendono indispensabili nuovi modulati approcci da parte degli organi istituzionalmente chiamati a contrastarle.

Résumé
Aujourd'hui le crime informatique est de plus en plus lié aux organisations criminelles transnationales qui ont développé de nouveaux modèles pour enrôler les personnes et pour obtenir des profits du recyclage de l'argent sale. Ces nouveaux types de crime, qui sont de plus en plus liés aux technologies informatiques sophistiquées, rendent nécessaire l'adoption de nouvelles stratégies de répression par les institutions.

Abstract
Today computer crime belongs to transnational criminal organizations which have new rules for the development of new strategies able to enrol people in their organizations and to obtain profits from money laundering. These new forms of crime which are more and more related to sophisticated data processing technologies must urge institutional agencies for new strategies against crime.

Nuove forme di criminalità connesse all'utilizzo dell'alta tecnologia informatica hanno recentemente assunto aspetti di vastissima importanza.

Il ben noto fenomeno del "phishing", le sempre più frequenti indebite utilizzazioni di carte di credito ed altri strumenti elettronici di pagamento hanno raggiunto oramai livelli di diffusione e pervasività tali da ingenerare fondate preoccupazioni nell'intero settore economico-finanziario anche in ragione del diffuso timore dell'insorgere di incontrollabili sensazioni di insicurezza nel foltissimo numero degli utenti.

Le nuove emergenze criminali stanno peraltro severamente impegnando le agenzie statuali di contrasto e repressione tese, in primis, alla più completa comprensione globale del fenomeno e quindi alla definizione dei più proficui connessi protocolli investigativi.

L'argomento sta ovviamente stimolando decisamente anche la comunità scientifica criminologica fortemente interessata da nuovissime riformulazioni dei tradizionali concetti delle tipologie di autore, dei profili vittimologici, dei variegati aspetti dei rapporti autore-vittima dell'illecito nonché delle innovative forme di schemi criminali associativi che si stanno via via evidenziando.

L'esperienza professionale di cui si vuol rendere testimonianza è stata prevalentemente maturata nel corso di una pluriennale attività operativa

• Direttore del Servizio Polizia Postale e delle Comunicazioni - Ministero dell'Interno - Dipartimento della Pubblica Sicurezza.

svolta nella Polizia Postale e delle Comunicazioni, una particolare Specialità della Polizia di Stato.

Le nuove imprese criminali.

Di indifferibile necessità appare a tal punto tracciare un sommario profilo delle nuove forme di criminalità informatica ricavato dalla concreta attività operativa svolta sul campo.

Un tempo esclusivo appannaggio di soggetti (ad esempio i noti hackers, i crackers ed altri) di elevate capacità tecnico-informatiche operanti in forma isolata ed autonoma e, molto spesso, senza alcuna diretta finalità di lucro, tali episodi criminali riconducono oggi, sempre più frequentemente, a composite organizzazioni che, ricorrendo alle più inusitate forme di arruolamento degli indispensabili esperti tecnici, gestiscono le fila di "imprese" che assicurano enormi introiti finanziari evidenziando nuovi modelli strutturali in ambiti decisamente transnazionali.

I nuovi crimini informatici.

Fondamentalmente incentrati nel cd furto di identità digitale (digital identity theft) i nuovi crimini sono precipuamente orientati verso il settore dei servizi bancari on line, la monetica (sistema monetario telematico costituito da carte di credito e dalla moneta elettronica in generale) ed il commercio elettronico.

Comune e sostanziale elemento caratterizzante è l'indebita appropriazione dei riservati dati personali che consentono l'accesso e la disponibilità di conti bancari on line, l'utilizzo di carte di credito o altri strumenti elettronici di pagamento.

Nel commercio elettronico il furto di identità è spesso utilizzato anche per commettere truffe a nome di ignare terze persone.

Si ritiene pacificamente che a gestire le fila di tali innovative attività criminali che assicurano i più elevati profitti col più basso rischio e che interessano l'intero mondo occidentale siano oramai gruppi criminali organizzati transnazionali.

Tra le più note aggressioni al sistema bancario on line risulta il cd. "phishing".

Migliaia di vittime all'anno vengono derubate delle riservate credenziali informatiche di accesso ai conti bancari o postali.

Ne conseguono poi ingenti illeciti prelievi per importi globali di milioni di euro.

Particolarmente sofisticati e originali si sono rilevati i sistemi di riciclaggio delle ingenti somme sottratte, imperniati in veri e propri arruolamenti on line di centinaia di gregari interessati alle complesse fasi di smaltimento del denaro senza lasciare traccia.

Alle centinaia di "soldatini" arruolati viene infatti chiesto di aprire conti on line di comodo su cui far confluire le somme asportate alle vittime.

Gli stessi "soldatini" vengono poi incaricati, incamerata una cospicua provvigione, di inoltrare generalmente le somme ricevute verso destinatari verso paesi dell'ex blocco sovietico, mediante ordinari servizi di transfer internazionali (Western Union – Money Gram).

Dalle indagini svolte è emerso che in quei Paesi è stata allestita un'altra speculare rete di gregari ricettatori che, ricevute le somme, le fanno pervenire ai boss delle organizzazioni.

Altre innovative forme di riciclaggio per lo più gestite da bande che, come ad esempio quelle rumene, possono contare su diffuse presenze sul territorio nazionale, prevedono lo "smaltimento" delle somme illecitamente ricavate attraverso

sistematiche "ricariche" di particolari carte elettroniche di pagamento di bancarie o postali (poste- pay e simili).

In alcuni forme più sofisticate il riciclaggio ha luogo attraverso ricariche di schede telefoniche prepagate che successivamente vengono utilizzate esclusivamente per chiamare numeri cd a tariffazione speciale o a valore aggiunto appositamente attivati.

L'esito sarà quello di percepire come provento del riciclaggio le percentuali nette del traffico telefonico attivato su quelle utenze speciali.

Evoluzione del fenomeno.

A meglio delineare l'evoluzione del fenomeno si porrà attenzione a tre fattispecie tipiche: il phishing, la monetica e le botnet.

- *il phishing*

Se in una sua prima fase il phishing era realizzato esclusivamente mediante invio di e-mail trappola tendenti cioè a ingannarne i destinatari e a carpire loro i riservati dati di accesso ai conti on line più recentemente esso è portato a termine mediante complesse tecniche di infezione informatica su larga scala di migliaia di computer.

Ad essere ingannati sono oramai le macchine, nuove vittime di temibili "virus informatici", propagati ad arte con la massima diffusione, che inducendo malfunzionamenti degli elaboratori, portano a far trapelare i riservati dati di accesso ai conti nella più totale inconsapevolezza degli utilizzatori.

Si hanno fondati motivi di ritenere che gli esperti informatici indispensabili per realizzare le sofisticate procedure tecniche del caso siano anch'essi oramai arruolati via internet da bande criminali di vasto spessore internazionale.

Nota è d'altro canto l'esistenza di un vero e proprio mercato nero dei virus informatici.

- *la monetica*

Anche il settore della monetica sta evidenziando radicali evoluzioni.

Oltre ai sempre più diffusi e gravi episodi di clonazione di carte di credito e di altri sistemi elettronici di pagamento, furti di milioni di riservati codici di carte di credito vengono oggi realizzati mediante attacchi informatici alle sempre più diffuse (e sempre più ricche!) banche dati che elaborano e gestiscono l'enorme flusso del commercio elettronico.

Le indagini in corso hanno evidenziato, con ampi riscontri, che composite bande criminali gestiscono ormai veri e propri mercati mondiali di riservati codici di conti bancari on line e di carte di credito.

- *le botnet*

Particolarmente temibili appaiono ancora le "botnet" (acronimo dei termini inglesi robot e network), vere e proprie new-entry nel panorama criminale informatico.

Le gang di cyber-criminali ostentano e misurano oggi la loro potenza in base alla vastità e alle dimensioni di reti (net) di computer violati (robot) di cui acquisiscono la disponibilità.

Queste "mandrie" di centinaia e, a volte migliaia, di macchine compromesse, abilmente gestite a distanza da capaci manovratori, vengono oggi utilizzate per realizzare gli attacchi informatici più arditi mascherandone totalmente la provenienza.

Pienamente funzionali, ad esempio, alla pratica del phishing e della diffusione di virus i computer violati continuano a restare nella apparente materiale disponibilità dei titolari del tutto ignari

che altri li utilizzano a loro insaputa per le azioni più nefande.

L'esperienza di polizia americana riporta già episodi di vere e proprie estorsioni realizzate tramite reti di computer zombi utilizzati per attaccare e danneggiare sistemi informatici aziendali per richiedere poi una sorta di pizzo informatico.

Dimensioni del fenomeno.

Le reali dimensioni del fenomeno risultano al momento difficilmente quantificabili anche in ragione delle ovvie resistenze dei settori finanziari interessati a fornire sia in ambito nazionale che internazionale precisi dati di rilevamento.

L'unico concreto riscontro è fornito dalle dimensioni del mercato nero mondiale dei dati riservati di conti bancari o di carte di credito oggettivamente rilevabili anche tramite Internet.

Sulla scorta delle analisi di una delle più note ed affidabili aziende mondiali di sicurezza informatica (Symantec) il volume potenziale dei dati offerti sul mercato nero ammonterebbe ad oltre 270 milioni di dollari nel solo periodo luglio 2007-giugno 2008.

Per quanto attiene alla monetica in generale, la più eloquente testimonianza della virulenza e dell'alto livello organizzativo delle aggressioni criminali di cui è fatta oggetto in ambito internazionale è fornita dalle più recenti note di cronaca che riferiscono di attacchi informatici a banche dati di aziende che gestiscono flussi di commercio elettronico con sottrazioni, in un solo episodio, di milioni di codici di carte di credito (si richiama il recente caso negli U.S.A. della Heartland Payment System).

I dati sono comunque in sensibile costante incremento di pari passo con la sempre più ampia informatizzazione di base del paese, la continua espansione del commercio elettronico, la sempre più incentivata diffusione di servizi bancari on-line e l'utilizzo generalizzato degli strumenti elettronici di pagamento ispirati dalla generalizzata "war cash".

Il quadro globale che si ricava porta a delineare i contorni di nuove imprese criminali che gestiscono in forme tutt'affatto innovative il business del malaffare informatico.

Raffinate menti le capeggiano abilmente sfruttandone appieno le enormi potenzialità economiche. La stesse "rete delle reti" Internet e le sue multiformi potenzialità relazionali (basti pensare alle stanze di chat, ai forum e alle sempre più frequentate reti di social network) sono il più pratico dei mezzi per selezionare e reclutare i migliori esperti di informatica, per entrare in disponibilità dei virus più raffinati.

Oltre a rendere estremamente agevole l'individuazione e l'assunzione dei tecnici la rete si presta anche, come anticipato, a favorire l'ingaggio degli addetti alle materiali operazioni di riciclaggio come nel caso del phishing.

I vecchi hacker o i cracker non appaiono più come i principali ed autonomi autori dei crimini informatici ma come meri prestatori d'opera a volte stabilmente inseriti nelle nuove imprese criminali, a volte ingaggiati all'occasione come ad esempio nel caso dei creatori di virus.

La chiara conoscenza e il più fattivo contrasto di tali emergenti imprese criminali richiedono oramai un imprescindibile approccio olistico che tenda a mutuare esperienze di alta investigazione in senso classico, di affinate capacità tecnico-

informatiche e non ultime, di consolidate capacità di orientamento nei complessi percorsi che presiedono alla movimentazione telematica dei flussi finanziari alla monetica ed al commercio elettronico.

Dal computer crime al computer related crime - L'apparente e la reale novità della criminalità informatica attuale.

Una più attenta riflessione sul crimine informatico (ora *computer related crime*) porta a scoprire la sua solo apparente novità.

Solo prima facie infatti il crimine informatico, nella sua attuale dimensione, si presenta come campo d'azione esclusivo di super tecnici che agiscono in totale autonomia sull'onda delle più recenti innovazioni dell'alta tecnologia informatica.

Il computer related crime, come in precedenza dettagliatamente analizzato, è oramai tornato saldamente "nelle mani" dei criminali di sempre.

Da abili burattinai essi muovono al meglio le loro schiere di marionette (tecnici informatici, riciclatori e gregari vari) secondo disegni criminali orientati all'esclusivo, ben noto scopo dell'illecito arricchimento.

Nuovi profili criminologici di autori e vittime.

Seppure ricondotte nell'alveo criminologico classico delle attività finalizzate al mero scopo di lucro tali nuove devianze evidenziano però alcune particolari connotazioni. In primo luogo il singolare rapporto tra boss e gregari. Molto spesso infatti, come sopra evidenziato, questi ultimi non hanno mai occasione di conoscere i primi.

Spiccatamente innovativo anche il rapporto autore-vittima che tale criminalità tende a configurare. Esempi tipici il phishing di ultima generazione che inganna le macchine all'insaputa dei titolari, i mercati neri globali dei codici di carte di credito carpiti da enormi banche dati, infine i tentativi di inganno su vasta scala indotti con l'invio massivo di milioni di e-mail trappola.

Appare in definitiva allontanarsi sempre più il diretto contatto tra criminale aggressore e vittima del raggiro profilandosi, per quel che attiene i manager delle organizzazioni, i netti contorni di una criminalità dei colletti bianchi di ultima generazione.

Nuove esigenze operative.

Sintetizzando quanto dettagliatamente delineato in precedenza la nuova criminalità informatica si prospetta con tipiche caratteristiche di impresa in cui boss con spiccate capacità manageriali arruolano ed ingaggiano in varia forma, facendoli ruotare intorno a sé a seconda delle necessità, da un lato tecnici esperti nell'allestimento di siti clone, nell'utilizzo di botnet, nella creazione e diffusione di malware e temibili virus e dall'altro stuoli di gregari con mansioni meramente esecutive destinati alle attività di monetizzazione degli ingenti proventi delle ruberie informatiche e quindi alla loro ricettazione e riciclaggio.

Una netta compartimentazione di ruoli contraddistingue la struttura cosicché molto spesso i gregari non sanno neanche chi sono i loro capi.

Le nuove imprese criminali, d'altro canto, non conoscono più limiti o barriere territoriali evidenziando anzi spiccati aspetti di transnazionalità.

Ogni adeguata risposta operativa non potrà non tenere conto di tali caratteristiche salienti.

Le attuali realtà operative in cui sono quotidianamente calati i cyber poliziotti della

Polizia Postale e delle Comunicazioni sembrano infatti suggerire la creazione di team di contrasto con una bilanciata compartecipazione di Agenti formati secondo schemi tradizionali e di altri con spiccate conoscenze tecnico-informatiche.

Oltremodo necessaria ed indispensabile si appalesa altresì una stretta e concreta sinergia con omologhe strutture investigative operanti in altri contesti nazionali.

Le strategie di contrasto dispiegate dalla Polizia Postale e delle Comunicazioni, organismo di Polizia di cui è stata di recente espressamente ribadita la esclusiva competenza a contrastare le varie fenomenologie del crimine informatico (decreto-legge 27 luglio 2005, n. 144 convertito in Legge 31 luglio 2005, n. 155) sono effettivamente orientate ad allestire funzionali gruppi operativi con dosata partecipazione di componenti con esperienze sia prettamente tecniche sia tipicamente investigative selezionati attraverso rimodulati schemi formativi.

Lo stesso organismo di Polizia sta peraltro sempre più perfezionando indispensabili ed estremamente proficui contatti con omologhi organismi operanti in altri contesti nazionali. Anche in tal senso è recentemente intervenuto un espresso riconoscimento normativo (Decreto del Ministro dell'Interno di concerto con il Ministro della Giustizia firmato a Roma il 24 novembre 2009) che ha visto individuato nel Servizio di Polizia Postale e delle Comunicazioni il cosiddetto "punto di contatto" in ambito G8 tra forze di Polizia straniere di ben 56 paesi per lo scambio dei flussi informativi nelle attività di Polizia contro il crimine informatico.